www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13268-13272

Detection and Prevention of Black Hole & Gray hole attack in MANET using Digital signature Techniques

Monika [1], ***Swati Gupta***[2]
[1]M.Tech Scholar,Geeta Institute of Management and Technology, Kurukshetra

monikamuradia@gmail.com

[2]Astt.Professor,Geeta Institute of Management and Technology, Kurukshetra

missbhasin@gmail.com

Abstract : ***A mobile ad-hoc network (MANET) infrastructure less dynamic network consists of collection of wireless mobile node that communicates with each other without the use of centralized network. Security in MANET is the most important concern for the basic functionality of network. The malicious node falsely advertises the shortest path to the destination node during the route discovery process by forging the sequence number and hop count of routing message . In this paper ,To avoid and remove this effect we will used Digital Signature Techniques .***

Keyword : MANET , AODV Protocol ,Black Hole Attack , Gray Hole attack , Digital Signature Technique.

I.INTRODUCTION

In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized .Due to absence of any kind fixed infrastructure and open wireless medium security implementation is difficult. In Manet each node function as a host as well as router, forwarding packets for another nodes in the network. MANET is vulnerable to various kind of attacks. These include active route interfering, imprecation and denial of service. Black hole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route REPLY (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. The malicious node launches this attack by advertising fresh route with least hop count and highest destination sequence number to the node which starts the route discovery .

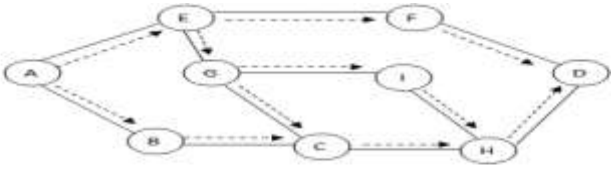

Fig 1: Route discovery process

II. AODV Protocol

The Ad-hoc on demand distance vector routing protocol is one of the widely used routing protocols in MANET. The route is established only when it is desired by the source node for data packets. Whenever node requires a route to the destination, a route discovery process is initiated. The source node floods the Route Request packet to its neighbours. The Route Request packet contains source identifier, destination identifier, source sequence number, destination sequence number, broadcast ID and TTL (Time to live). The intermediate node either forwards the packet or prepares a Route Reply if it has a fresh or valid route to the destination. This validity is determined by comparing the sequence number of intermediate node with the destination sequence number of Route Request packet. The destination node or the intermediate node that has the freshest route sends the Route Reply message back to the source node in the reverse path .

2). The source node receives many Route Reply packets and the fresher and shorter path is selected to send the data packet packet .

III (a) . Black Hole attack

The Black hole attack in MANET is very serious problem . It affect the security in MANET .During the route discovery process it shows the highest destination sequence number . It shows the shortest path towards the destination . Source node will select this shortest path from this node towards destination . Then source node will send the packet to this node . It will drop or consume that packet and don’t allow to forward towards next node . As the result of this , Packet delivery ratio , Throughput , end to end delivery ratio will decrease . In this paper ,to avoid this defect I have tried to detect then prevent this defect using digital signature techniques .

Single Black Hole Attack :

AODV route discovery mechanism is based on RREQ/RREP messages. Source node broadcasts the RREQ message to its neighbors. Either the destination or intermediate node sends RREP. The RREP received first by source node is accepted and all further RREPs are discarded. Black hole node takes benefit of this feature of AODV and sends RREP first even without checking its routing table. In this way, a route through black hole node is setup and black hole node consumes all the forwarded packets

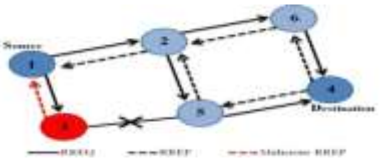

Fig 2: Single Black Hole Attack

In figure ,node 3 is black hole node through which final route is established. Being the black hole node, it consumes all the packets without forwarding them.

B. Cooperative Black Hole Attack

Cooperative Black hole means the malicious nodes act in a group . As an example,

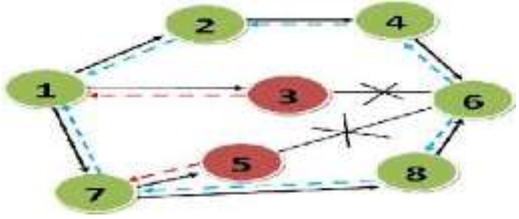

Fig 3: cooperative black hole attack

In above Example, when multiple black hole nodes are acting in coordination with each other, the first black hole node 3 refers to one of its teammates node 5 as the next hop, .The source node 1 sends a “Further Request (FRq)” to 5 through a different route (1-7-node 5) other than via 3. Node 1 asks node 5 if it has a route to destination node 6. Because node 5 is cooperating with node 3, its “Further Reply (FRp)” will be “yes” to both the questions, then all the packets are consumed by node 3 and don’t allow it to further proceed.

III (b) Gray Hole attack

Gray Hole attack is a variation of the black hole attack in which the malicious node may behave as an honest node first during the route discovery process and then may change its state to malicious and vice versa. This malicious node may then drop all or some of the data packets. The gray hole attack is difficult to detect due to congestion, overload and also due to malicious nature and ability of changing states. Instead it behaves as an honest node and when data packets arrive through this path, it drops all the data packets. A condition is added to drop all the data packets if it is not the destination otherwise receive all the data packets. Gray hole node act honest node during route discovery process but in actual it is an attacker .

- Dropping all UDP packets while forwarding TCP packets.

- Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures

IV. Problem Statement

Black hole node as well as Gray hole node created the problem in the MANET . Secuirty is important concern in all kind of network . Ad-hoc wireless networks are highly vulnerable to security attacks as compared to other wired networks. This is due to the following characteristics: insecure operating environment, physical vulnerability, shared broadcast radio channel, lack of central authority, limited availability of resources . Malicious node act as a barrier in the secure path As it will absorb the data and thus reduce packet delivery , degrade the performance , Decrease end to end delivery , decrease throughput. To secure a network to detect and avoid it very important task .

V. Proposed Solution

In this Dissertation , to detect and prevent malicious node , Digital signature techniques used which is a verification techniques .this technique is used to validate the authenticity and integrity of message , software and document Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message . Digital signatures rely on certain types of **encryption** to ensure authentication. Encryption is the process of taking all the data that one node is sending to another and encoding it into a form that only the other node will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signature . In this paper , this technique plays a very good role to detect and prevent the defect . All of the node that exist in the network have legitimate digital signature .whenever a node require route to destination route discovery process will take place .Source node will broadcast the route request packet to all of the neighbour node . The Route Request packet contains source identifier, destination identifier, source sequence number, destination sequence number, broadcast ID . the intermediate node will either forward this request to next node or prepare a route reply packet if it will have valid route to destination .digital signature technique will work at the time of route reply . whenever source node will get the route reply packet from intermediate node it will verify this node with the help of its node id .as all of the node existing in the network have its unique node- id by which it is uniquely identified and it is registered on trust based server .when intermediate node will send the route reply packet to source node this packet will contain data or information and node id of the node which is unique for each and every node . source node will send it to trust based server to check whether this packet come from authenticate node or not . Trust based server will check its encryption key whether its registered or not . if its registered then there will be no issue it can be a route towards destination but if it does not match then it means it is malicious node or an attacker which is identified by trust based server . Thus we will detect this node ,source node will broadcast the message in between all that node that node having particular id is malicious node . then all of the node will not consider the path in which such kind of node occur at the time of discovery process .then it will consider another path and will ignore this one .Thus , we will prevent this .

Algorithm :

```
Algo ( malicious _ node _detection)
Input: no. of nodes n, Source node, Destination Node;
Output: Detection and prevention of Attacker, Find the Best Path for routing;
Begin Create the network for the input node (of n number nodes)
Define Source node & Destination Node
Find the neighbours node of source node ;
For source to destination
Send Route Request to neighbour nodes for finding the destination;
If next node is destination
Then direct path is established
Else
Broadcast the RREQ to next neighbours
End for
For  destination to source
Select the shortest path with minimum no. Of nodes
RREP to pervious node with digital signature
Transfer digital signature  to trust based server for verification
if digital signature matched
then  destination is legal ,Establish a path for data transfer.
Else
Destination is not legal
Then add the malicious node information in malicious node column and spread this information in whole network;
again rebroadcast Route request (RREQ)
End for
End
```

VI. Simulation Result

The model is simulated using MATLAB R 7.10 a .

As in the below figure , No. of nodes are distributed in the network . Due to dynamic characteristics of Manet all of the node can move randamolly from one position to another .Let node 19 is source node whereas node 36 is destination node . Node 19 will broadcast route request in the network. Node 7 will forward this packet furtherlly. node having red star indicate that particular node is malicious node in the path.This network having multiple malicious node. Node 42 is malicious node in the path . As this node will occur in path source node detect this node using its digital signature as describe previously . Source node will avoid this path for data propagation and packet will forward from node 7 to node 17 when RREP packet come from node 17 then digital signature will be verify and if it is valid node then it mean it is best route towards destination and this process going on until not reach at destination.

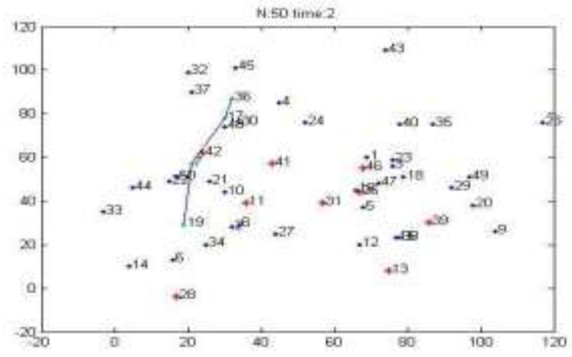

Fig 5 : Network consist of 50 nodes

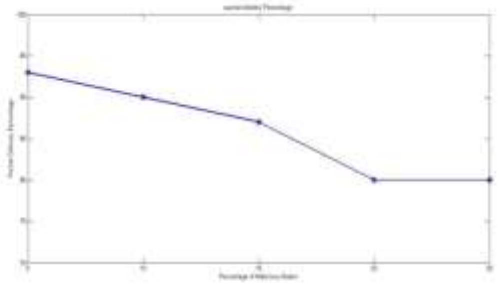

Fig 6 : Packet delivery Vs. No. Of malicious nodes

In the above Fig 6 , it is shown that by increasing the no. of node no. of packet deliver will decrease.

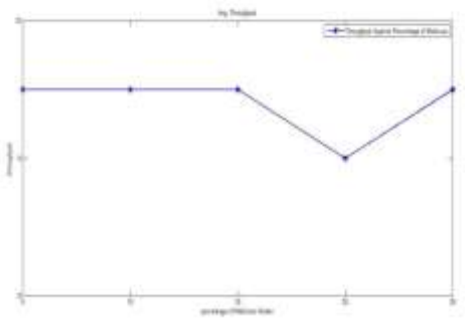

Fig 7 : Throughput Vs. No. Of malicious nodes

In the above Fig 7 , it is shown that by increasing the no. of nodes throughput will be decreased. Intially , it is constant but as malicious node occur in the path it is abruptly decrease.

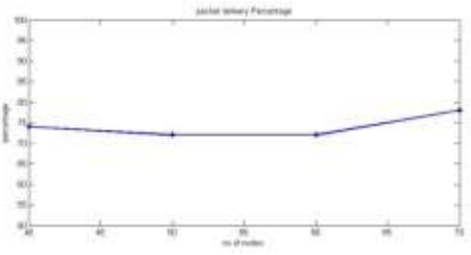

Fig 8: Packet delivery without Digital Signature

Above graph shown that without digital signature no. of packet deliver will be reduce .

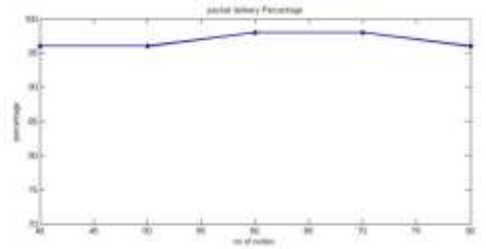

Fig8 :Packet delivery with Digital Signature

Above Graph shown that with digital signature ,no. of packet deliver will be increased and packet delivery will be increased.

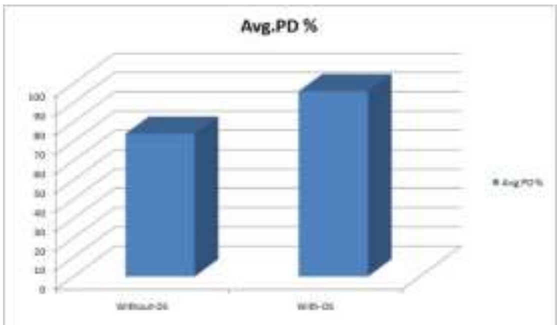

Fig 9 : Graph Comparison with and without digital signature

Above graph shown that without digital signature verification techniques , Packet delivery is around 75% else while with digital signature verification techniques Packet delivery is around 95% .

VII. Conclusion and Future Scope

This research has provided efficient technique to solve the problem arising from such attack . Security is main concern in each wireless network . Due to some characteristics of Manet such as dynamic nature , infrastructure less , mobility there is big influence on security . Using some verification technique we can avoid these attack .

In this paper we have presented a feasible solution to detect 2 types of malicious nodes(Black/Gray Hole) in the ad hoc network. The proposed solution can be applied to identify and remove any number of Black Hole or Gray Hole Nodes in a MANET and discover a secure path from source to destination by avoiding the above two types of malicious nodes. In the future we will try to enhance packet delivery ratio , throughput and decrease packet dropped ratio and to improve performance .

REFERENCES

[1] D. Djenouri, L. Khelladi and N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," IEEE Commun. Surveys and Tutorials, vol. 7, no. 4, pp. 2-28, 2005.

[2] S. Desilva, and R. V. Boppana, “Mitigating Malicious Control Packet Floods in Ad Hoc Networks,” Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[3] M. G. Zapata, "Secure Ad Hoc on-demand Distance Vector (SAODV) Routing," IETF Internet Draft,draft-guerrero-manet-saodv-03, 2005,

[4] F.-H. Tseng, L.-D. Chou, and H.-c. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Human-centric Comput. In! SCi., vol. I, no. I, p. 4, 2011.

[5] Hoang Lan Nguyen , Uyen Trang Nguyen "A Study of different types of attacks in mobile adhoc networks ", Department of Computer Science and Engineering, pp. 2-7, 2012 .

[6] A. M. Kanthe, D. Simunic, and R. Prasad, "Eflects of malicious attacks in mobile ad- hoc networks," 2012 IEEE Int. Conf. Comput. Intell. Comput. Res., pp. 1-5, Dec. 2012 accessed on 20 Jan 2013

[7] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad HocinMANET”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3,September 2011, PP:Network,” IEEE Com

[8] Jagdish J. Rathod , Amit Lathigara,” Novel Approach of Preventing and Detecting Gray Hole Attack on AODV based MANET”, Volume 3, Issue 1, January 2015

[9] Sandeep Kumar, Mrs. Sangeeta Pramod Kumar Soni,” A Review on Gray Hole Attack in MANETs”, Volume 4, Issue 9, September 2014

[10] “An Efficient Wormhole Prevention in MANET Through Digital Signature” Anil Kumar Fatehpuria1, Sandeep Raghuwanshi, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March 2013)

[11] A.Vani, D.Sreenivasa Rao, ”Removal of Black Hole Attack in Ad Hoc Networks to provide confidentiality Security Service”, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 3, March 2011.

[12]Pooja , Vinod kumar ,” A Review on Detection of Blackhole Attack Techniques in MANET’’International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, issue 4, pp.364-368, 2014

[13]Neeraj saini , lalit Garg ,” Enhanced AODV Routing Protocol against Black hole Attack’’,International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, issue 6, pp.847-850, June 2014

[14]Kriti Chadha , Dr. Sushmita Jain ,’’Impact Of Black Hole And Gray Hole Attack In AODV Protocol “,IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India

[15]. Asha Guddadavar , Bagali Ashvini A ‘’ Black Hole detection and avoidance in mobile Adhoc Networks’’, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 5 May 2015, Page No. 11854-11858.

[16] Gurnam Singh, Gursewak Singh ‘’ Detection and Prevention Of Black Hole Using Clustering In MANET Using Ns2’’ International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume - 3 Issue -8 August, 2014 Page No. 7420-7430.

[17] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," vol. 5, no. 3, pp. 338-346, 2007.

[18] Mahesh Kumar Kumawat, Jitendra Singh Yadav,” A Survey on Detection and Prevention Techniques for Gray-Hole Attack in MANET”,) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1288-1290.